December 2021

ITI Cyber Action Plan: Infrastructure Implementation Recommendations for State and Local Governments

Government entities face an increasingly sophisticated range of cybersecurity threats, and state and local governments are particularly susceptible to criminal hackers given the amount of sensitive information they store, the number of access points to IT systems, and the aging IT infrastructure. The Infrastructure Investment and Jobs Act includes significant levels of new resources aimed at making state and local information systems more resilient. ITI offers the following recommendations to state and local governments as they prioritize and invest the resources from the Infrastructure Investment and Jobs Act including in both broadband buildout plans and requests for cyber specific grants:

Adopt New Cyber Technologies. State and local governments should adopt commercial IT products. If there are government-specific needs, they should first look to utilize existing federal standards and not impose their own government-unique requirements on IT products to the greatest extent possible. This is the best way to ensure governments have access to up-to-date cybersecurity measures and safeguards and can assist state and local governments in bolstering their defenses. Typically, these technologies carry commercial terms and conditions required to allow the technologies to work efficiently and be installed quickly. When technologies are not properly updated or maintained, as is often the case when governments eschew commercial products in favor of building out their own IT infrastructure, this can increase a system's susceptibility to cyberattacks and in turn result in long-term losses.

Prioritize IT Modernization and Secure Line-Item Budget Funding to Support this Investment. According to the National Conference of State Legislatures (NCSL) research, out of 100 leading legislators polled, 45 percent picked IT modernization as the most important IT-related policy issue at the state and local levels because of the SolarWinds cyber attack and COVID-19.[1] Moreover, these legislators are interested in the industry's assistance to understand the issue further.[2] Nevertheless, IT modernization continues to lag in terms of funding to support such investment.

Support Funding for Cyber Education and Training. Governments should support an increase in federal funding for cyber defense capabilities, cybersecurity education, training, and skills development programs for state and local employees. According to a U.S. Department of Commerce and Department of Homeland Security report, *Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce*, "employers increasingly are concerned about the relevance of cybersecurity-related education programs in meeting the needs of their organizations." As cyber threats continue to grow in sophistication, states face a persistent challenge in recruiting skilled cybersecurity professionals and training employees capable of protecting their systems against the threat of malicious actors. With cybercriminals now responsible for billions in losses per year, the need for individuals qualified to secure networks against attackers has never been greater.

Adopt Federal Cyber Standards and Collaborate with Federal Partners. The federal government has made a significant investment in developing cybersecurity best practices, procurement standards, and information sharing platforms to combat cybersecurity risks to governments. The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) is the collective product of public and private stakeholders and offers a flexible approach to managing cybersecurity risks. These technology-agnostic best practices and standards which help create consistency across government agencies and avoid duplication of standards across various federal agencies, offer the same benefit to state and local agencies. In order to adopt these standards, state and local entities should assess their risk as per the CSF and take appropriate measures to implement best practices that enhance cyber preparedness and response capabilities. This includes requiring state and local governments to understand the data they collect and store and develop safeguards to protect this data. These policies should be reviewed and updated regularly in keeping with federal standards and requirements.

Adopt Cloud Solutions and Recognize Pre-Existing Compliance Regimes for IT Vendors. Amid the rapid pace of innovation and digital transformation, utilizing cloud computing services can reduce IT costs, provide a more secure data storage environment, improve speed and bandwidth on existing systems, and ease the burden on in-house IT management. By leverage pre-existing security baselines for assessing cloud service providers and adopting commercial cloud solutions, governments rapidly modernize their IT while eliminating the costs to taxpayers associated with building and maintaining those IT products. In order to quickly deploy secure cloud solutions, state governments should allow for reciprocity with compliance regimes like NIST 800-171 and the Federal Risk and Authorization Management Program (FedRAMP) if conducting their own authorization process.

Support DHS State and Local Cybersecurity Programs. State and local entities are the first line of defense in protecting relevant proprietary citizen data and information. In a 2020 report by the Cyberspace Solarium Commission, they recognized the federal government's central role and the Cybersecurity and Infrastructure Security Agency (CISA) in working with states and partners outside of the federal government to enhance cybersecurity practices. To support a whole of government approach with all relevant stakeholders, states and local entities must have a seat at the table. The implementation of the new U.S. Department of Homeland Security State and Local Cybersecurity Grant Program included in the Infrastructure Investment and Jobs Act will provide grants to state and local governments to develop and implement comprehensive cybersecurity plans and address imminent cybersecurity threats**.**

Develop Robust Incident Response and Recovery Plans. As the number and severity of cyber intrusions have increased, IT departments have realized that every minute counts when it comes to an effective response. Cybercriminals are able to do the greatest damage when their attack goes unnoticed or when it is noticed there is not a clear plan with clearly defined roles in place to respond. Per the NIST Cybersecurity Framework, state and local governments must have robust critical incident response plans that ensure cyberattacks are addressed in real-time and limit the damage. This includes providing funding for tabletop exercises and ensuring that vendors have access to state and local cybersecurity professionals at all times**.**